REMARKS

In the office communication mailed September 26, 2007, claims 17 and 18 are rejected under 35 U.S.C. §103(a) given Nakahara (U.S. Patent No. 5,594,429) ("Nakahara") in view of Gullman et al. (U.S. Patent No. 5,280,527) ("Gullman"). Claims 17 and 18 have been amended to overcome the rejection. Thus, the Applicants hereby respectfully traverse the rejections and request reconsideration.

Rejections Under 35 U.S.C. §103

Claims 17-18 were rejected under 35 U.S.C. §103(a) given Nakahara in view of Gullman. Prior to addressing the merits of the Examiner's rejection, the Applicants believe it would first be helpful to briefly describe and characterize the Nakahara and Gullman references.

Nakahara describes a system for transmitting and receiving security and function information. A variable code may be transmitted from a transmitter to a receiver along with a fixed code. The receiver determines whether the fixed and variable codes are valid and an ***exact*** match is required for validity to be established. More specifically, Nakahara requires that "the received ID code ***coincides*** with the identification information stored in the receiver."[1] The Examiner acknowledges that Nakahara does not describe an encryptor.

Gullman FIG. 1 (reproduced below) shows an overview of a general security system.

[1] See Nakahara, Col. 6, lines 20-21.

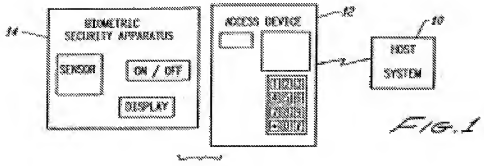
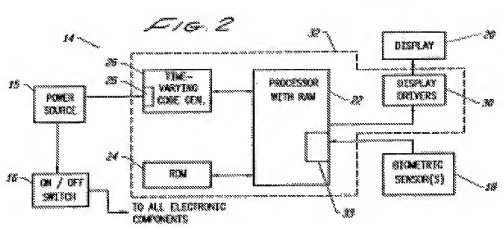


FIG. 1

A security token is created at a security apparatus 14 and the token includes a fixed code and a "time-varying code."[2] These codes are transmitted from a security apparatus 14 to an access device 12 and then to a host system 10. When received at the host 10, the token is decoded.[3] A match between the codes transmitted by the security apparatus 14 and the host system 10 is required. More specifically, Gullman states that "[t]o properly decode the token, the security apparatus 14 is ***synchronized*** with the host system 10 so that the time varying code is ***identical*** at both the security mechanism 14 and the host system 10."[4]

Moreover, Gullman also varies his codes with time as seen in FIG. 2 (reproduced below). Specifically, within the security apparatus 14, these time varying codes are created by a time varying code generator 26 where the time-varying code is ultimately based on the time of day.[5]

[2] Gullman, Col. 3, lines 38-42.
[3] Gullman, Col. 3, lines 36-44.
[4] Gullman, Col. 4, lines 23-26 (emphasis added).
[5] Gullman, Col. 5, lines 4-5.



Claim 17

Claim 17 has been amended to recite the language of encrypting a fixed code "*independent of time*" and which varies instead with actuation of the transmitter. This limitation is neither disclosed in nor obvious in view of Nakahara and Gullman.

As stated above, the Examiner acknowledges that Nakahara does not disclose an encryptor and Gullman merely discloses encryption through the use of a *time*-varying code. Specifically, Gullman's time-varying code is based on the time of day and is not affected by the actuation of a transmitter; that is, Gullman's code varies only as a function of time and not with the number of times that the transmitter is actuated.

The Applicants disclose a rolling or variable code that remains independent of time and changes instead with each actuation of the transmitter.[6] Specifically, the Applicants disclose a method of encryption using a transmitter that includes a means for producing a 32-bit frame comprising the variable portion of the code. When the transmitter is actuated, then the 32-bit rolling code is mirrored to provide a 32-bit

[6] Farris at 0009.

mirrored rolling code. The 32-bit mirrored rolling code then has its most significant bit "deleted" and it then converts the 32-bit mirrored code to a trinary bit rolling code.[7]

Hence, the process of encryption surrounding the rolling or variable code clearly remains independent of time and is instead affected by the actuations of the transmitter; i.e., the number of times the transmitter is actuated. For example, at t=0, the transmitter can be actuated to produce a specific encrypted code X. If the transmitter is not actuated, then at t=1 day, the specific encrypted code would *still* be X. Likewise, if the transmitter is not actuated until t=3 months, the specific encrypted code would *still* in fact be X. It is therefore clear, both implicitly and explicitly from the specification, that since encryption is only effected as a function of the actuations of the transmitter and that the passing of time itself has no effect whatsoever on the encryption result, the encryption process is independent of time. Thus, there is proper support within the specification for teaching encryption that is "independent of time."

Claim 18

Claim 18 recites a receiver (compared to the transmitter in claim 17) and includes recitations similar to claim 17. Consequently, it is submitted that claim 18 is allowable over the proposed combination for the same reasons as claim 17. The Applicants therefore respectfully submit that claim 18 is not obvious for a variety of reasons, including those expressed above.

[7] Farris at 0009.

CONCLUSION

There being no other objections to or rejections of the claims at this time, the Applicants respectfully submit that claims 17 and 18 may now be passed to allowance.

The Commissioner is hereby authorized to charge any additional fees which may be required with respect to this communication, or credit any overpayment, to Deposit Account No. 06-1135.

Respectfully submitted,

FITCH, EVEN, TABIN & FLANNERY

Dated: December 26, 2007

Steven G. Parmelee
Registration No. 28,790

120 South LaSalle Street, Suite 1600
Chicago, Illinois 60603-3406
Telephone (312) 577-7000
Facsimile (312) 577-7007
498974